

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
12 May 2005 (12.05.2005)

PCT

(10) International Publication Number
WO 2005/043281 A3

(51) International Patent Classification⁷: H04L 29/06,
29/12

(21) International Application Number:
PCT/JP2004/016708

(22) International Filing Date:
4 November 2004 (04.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003-374880 4 November 2003 (04.11.2003) JP
2004-034172 10 February 2004 (10.02.2004) JP
2004-037314 13 February 2004 (13.02.2004) JP

(71) Applicant (for all designated States except US): NTT COMMUNICATIONS CORPORATION [JP/JP]; 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP).

(72) Inventors; and

(75) Inventors/Applicants (for US only): SAITO, Makoto [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). TOKUNAGA, Osamu [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). YAMASAKI, Toshiyuki [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). MIYAKAWA, Shin [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). SHIRASAKI, Yasuhiro [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). UCHIYAMA, Takamasa [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). FUKADA,

Satoshi [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). EGASHIRA, Takashi [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP). SUZUKI, Toshiaki [JP/JP]; c/o NTT COMMUNICATIONS CORPORATION, 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 1008019 (JP).

(74) Agent: ITOH, Tadahiko; 32nd Floor, Yebisu Garden Place Tower, 20-3, Ebisu 4-chome, Shibuya-ku, Tokyo 1506032 (JP).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

(88) Date of publication of the international search report:
18 August 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A3

WO 2005/043281

(54) Title: METHOD, APPARATUS AND PROGRAM FOR ESTABLISHING ENCRYPTED COMMUNICATION CHANNEL BETWEEN APPARATUSES

(57) Abstract: A method for establishing an encrypted communication channel between a first apparatus and a second apparatus by using a session management apparatus is disclosed. The method includes the steps of: establishing a first encrypted communication channel between the session management apparatus and the first apparatus by performing mutual authentication between the session management apparatus and the first apparatus; establishing a second encrypted communication channel between the session management apparatus and the second apparatus by performing mutual authentication between the session management apparatus and the second apparatus; and exchanging key information between the first apparatus and the second apparatus via the first encrypted communication channel and the second encrypted communication channel so as to establish an encrypted communication channel between the first apparatus and the second apparatus.